Billing Code:

OFFICE OF MANAGEMENT AND BUDGET

Proposed Designation of Databases for Treasury's Working System under the Do Not Pay Initiative

AGENCY: Office of Management and Budget.

ACTION: Notice of Proposed Designation.

SUMMARY: Section 5(b)(1)(B) of the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA) provides that the Director of the Office of Management and Budget (OMB), in consultation with agencies, may designate additional databases for inclusion under the Do Not Pay (DNP) Initiative. IPERIA further requires OMB to provide public notice and an opportunity for comment prior to designating additional databases. In fulfillment of this requirement, OMB is publishing this Notice of Proposed Designation to designate the following six databases: 1) the Department of the Treasury's (Treasury) Office of Foreign Assets Control's Specially Designated Nationals List (OFAC List), 2) data from the General Services Administration's (GSA) System for Award Management (SAM) sensitive financial data from entity registration records (including those records formerly housed in the legacy Excluded Parties List System), 3) the Internal Revenue Service's (IRS) Automatic Revocation of Exemption List (ARL), 4) the IRS's Exempt Organizations Select Check (EO Select Check), 5) the IRS's e-Postcard database, and 6) the commercial database American InfoSource (AIS) Deceased Data for inclusion in the Do Not Pay Initiative. This notice has a 30-day comment period.

DATES: Please submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. At the conclusion of the 30-day comment period, if OMB decides to finalize the designation, OMB will publish a notice in the Federal Register to officially designate the database.

ADDRESSES: Comments must be submitted electronically before the comment closing date to www.regulations.gov. The public comments received by OMB will be a matter of public record and will be posted at www.regulations.gov. Accordingly, please do not include in your comments any confidential business information or information of a personal-privacy nature.

FOR FURTHER INFORMATION CONTACT: Brian Nichols at the OMB Office of Federal Financial Management at 202-395-3993.

SUPPLEMENTARY INFORMATION:

Among other things, IPERIA codified the DNP Initiative that was already underway across the Federal Government. The DNP Initiative includes multiple resources to help Federal agencies review payment eligibility for purposes of identifying and preventing improper payments. As part of the DNP Initiative, OMB designated Treasury to host Treasury's Working System, which is the primary system through which Federal agencies can verify payment eligibility.

Pursuant to IPERIA,[1] OMB has the authority to designate additional databases for inclusion in the DNP Initiative.[2] OMB Memorandum M-13-20[3] provides guidance related to IPERIA and explains the process by which OMB will consider designating additional databases. The OMB guidance provides that OMB will only consider designating databases that are relevant and necessary to meet the objectives of section 5 of IPERIA. In addition, the guidance explains that six factors will inform OMB when considering additional databases for designation. These factors include: 1) statutory or other limitations on the use and sharing of specific data; 2) privacy restrictions and risks associated with specific data; 3) likelihood that the data will strengthen program integrity across programs and agencies; 4) benefits of streamlining access to the data through the central DNP Initiative; 5) costs associated with expanding or centralizing access, including modifications needed to system interfaces or other capabilities in order to make data accessible; and 6) other policy and stakeholder considerations, as appropriate.

For commercial databases, the OMB guidance establishes additional requirements. The guidance requires that the commercial data meet the following general standards: 1) information in commercial databases must be relevant and necessary to meet the objectives described in section 5 of IPERIA; 2) information in commercial databases must be sufficiently accurate, up-to-date, relevant, and complete to ensure fairness to the individual record subjects; and 3) information in commercial databases must not contain information that describes how any individual exercises rights

[1] 31 U.S.C. § 3321 note, Pub. L. 112-248 (2013).
[2] OMB designated the Department of the Treasury to host Treasury's Working System, which helps Federal agencies verify that their payments are proper. Treasury's Working System is part of the broader DNP Initiative.
[3] "Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative" - August 16, 2013.

guaranteed by the First Amendment, unless use of the data is expressly authorized by statute. In addition, when OMB designates commercial databases for use in Treasury's Working System, Treasury must meet the following specific requirements: 1) Treasury shall establish rules of conduct for persons involved in the use of, or access to, commercial databases and instruct each person with respect to such rules, including penalties for noncompliance, as appropriate; and 2) Treasury shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of information in commercial databases when such information is under Treasury's control.

Considerations for Designating the Office of Foreign Assets Control's Specially Designated Nationals List (OFAC List)

OMB proposes to designate the Treasury OFAC List for inclusion in Treasury's Working System. Acting under Presidential national emergency powers, the Office of Foreign Assets Control (OFAC) derives its authority from a variety of U.S. Federal laws regarding embargoes and economic sanctions such as those terrorism-related mandates found in 31 C.F.R. Parts 595-597. This database is a list of persons and entities whose assets are blocked and generally prohibited from entering into financial transactions with United States (U.S.) financial institutions and the U.S. Government.

Currently, each payment-issuing agency has its own procedure for blocking or rejecting payments to persons or entities on the OFAC List. By designating the OFAC List as an additional database in Treasury's Working System, Treasury would improve

and streamline access by allowing agencies to verify payment eligibility at multiple points in the payment process.

OMB has reached the following initial determinations and is seeking public comment before finalizing the designation of the database.

1. There are no statutory or other limitations that would prevent including this public database within Treasury's Working System for the purposes of verifying payment eligibility. Due to the broad audience of government agencies required to check OFAC's List, this database was made accessible to agencies matching against Treasury's Working System soon after IPERIA became effective and before the issuance of OMB Memorandum M-13-20 establishing this designation process. The database is formatted for information processing on OFAC's website and requires no changes to existing processes or any additional expense for Treasury.

2. There are no prohibitive privacy restrictions or risks for Treasury to make this publicly facing database already available on OFAC's website also available in Treasury's Working System. Risk mitigation measures include maintaining a current and compliant Security Accreditation and Authorization (SA&A) package for Treasury's Working System in accordance with OMB Circular No. A-130, Managing Information as a Strategic Resource, and complying with the Federal Information Security Modernization Act (FISMA) requirements. To reduce the likelihood of incidents triggered by unauthorized access, login to Treasury's Working System requires public key infrastructure (PKI) or personal identity verification (PIV) credentials. All users and administrators are required to sign rules of behavior stipulating their responsibilities to minimize risks and support DNP's mission to "Protect the integrity of the government's

payment process by assisting agencies in mitigating and eliminating improper payments in a cost-effective manner while safeguarding the privacy of individuals." In this vein, Treasury has also dedicated resources to establish a Privacy Program based on applicable requirements, the Fair Information Practice Principles (FIPPs), and industry best practices. Treasury's Privacy Program champions various internal controls in concert with agency leadership and counsel such as a data usage governance process charged with vetting projects that support a data driven approach to reducing improper payments for Treasury's specific customers and government-wide.

3. Designating the OFAC List would likely strengthen program integrity. With access to the OFAC List through Treasury's Working System, an agency will be better equipped to minimize the risk that it makes a payment to a person or entity on the list and the potentially catastrophic impact of such a payment.

4. It would be beneficial to streamline access to the OFAC List through its inclusion as an additional database within Treasury's Working System. IPERIA requires agencies to check the Act's enumerated databases prior to making a payment with Federal funds. Federal regulations, such as 31 C.F.R. Parts 595-597, require paying agencies to check the OFAC List. Many of DNP's customers are paying agencies that are required to check the OFAC List. They will now be able to check it along with the other databases that comprise Treasury's Working System. This will enable agencies to make more informed payment decisions, increase efficiency, and strengthen internal controls.

5. There are no additional costs associated with expanding or centralizing access to the OFAC List within Treasury's Working System.

6. No additional stakeholder considerations were identified. Regarding policy, the designation further ensures that Treasury customers adhere to terrorism-related mandates set forth in Federal regulations, such as those found in 31 C.F.R. Parts 595-597.

Considerations for Designating System for Award Management (SAM) Sensitive Financial Data from Entity Registration Records

OMB proposes to designate SAM sensitive financial data from entity registration records specifically the sensitive financial data and exclusion data for use in the DNP initiative via Treasury's Working System. SAM is the single registration point for entities seeking Federal contracts or grants (with limited exceptions defined in the Federal Acquisition Regulation (FAR) or Title 2 of the Code of Federal Regulations). As such, key data that are essential to appropriately identifying unique entities for DNP are included in the entity registration records in SAM and identified as sensitive data, meaning they are not disclosed publically. These data include information used in financial transactions.

By designating SAM sensitive financial data from entity registration records as an additional data source in DNP via Treasury's Working System, agencies using the system will have greater confidence in results returned from the Treasury Working System and used in analysis for processing payments. This would reduce the administrative burden for agencies having to check both systems prior to finalizing pre- and post-payment analysis.

OMB has reached the following initial determinations and is seeking public comment before finalizing the designation of the database.

1. There are no statutory or other limitations that would prevent the DNP Initiative from using SAM sensitive financial data from entity registration records for the purposes of verifying payment eligibility. GSA is authorized to maintain SAM pursuant to the FAR Subparts 4.11, 9.4, 28.2, and 52.204, 2 C.F.R. Part 25, and 40 U.S.C. 121(c), and the data collection requirements from entities is governed by the FAR and Title 2 of the Code of Federal Regulations. The records in SAM sensitive financial data from entity registration records are covered by a Privacy Act system of records. Pursuant to the system of records notice's (SORN)[4] routine use (m), GSA is permitted to disclose SAM sensitive entity registration data for the purposes of the DNP Initiative. DNP currently receives SAM sensitive financial data from entity registration records and comports with the GSA routine use when re-disclosing the data to Federal agencies 'for the purpose of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state in a state-administered, federally funded program' (78 FR 11648, Feb. 19, 2013). Adding this data source to the DNP Initiative will not require any additional action because this database was made accessible to agencies for DNP soon after IPERIA became effective and before the issuance of OMB Memorandum M-13-20 establishing this designation process and Treasury's Working System.

2. There are some privacy restrictions and risks associated with the DNP Initiative's use of the SAM sensitive entity registration data. For example, SAM is a system of records, so the Privacy Act governs the DNP Initiative's use of these records. As mentioned above with respect to the first consideration, DNP would comport with the SORN's

[4] SAM SORN: http://www.gsa.gov/portal/mediaId/205455/fileName/2013-03743.action

routine use (m), which mitigates the privacy risks with respect to the Privacy Act. Risk mitigation measures also include maintaining a current and compliant SA&A package for Treasury's Working System in accordance with OMB Circular No. A-130 requirements. To reduce the likelihood of incidents triggered by unauthorized access, login to Treasury's Working System requires PKI or PIV credentials. All users and administrators are required to sign rules of behavior stipulating their responsibilities to minimize risks and support DNP's mission to "Protect the integrity of the government's payment process by assisting agencies in mitigating and eliminating improper payments in a cost-effective manner while safeguarding the privacy of individuals." In this vein, Treasury has also dedicated resources to establish a Privacy Program based on applicable requirements, FIPPs, and industry best practices. Treasury's Privacy Program champions various internal controls in concert with agency leadership and counsel such as a data usage governance process charged with vetting projects that support a data driven approach to reducing improper payments for Treasury's specific customers and government-wide.

3. Designating SAM sensitive financial data from entity registration records would strengthen program integrity. With SAM sensitive financial data from entity registration records as a data source in DNP, agencies would have more convenient access to these data, strengthening their ability to make stronger and more efficient payment determinations and reducing false positives that result in improper withholding of or late payments.

4. It would be beneficial to streamline access to SAM sensitive financial data from entity registration records as an additional database within Treasury's Working System. Many

of Treasury's Working System users are payment-issuing agencies that are required to check SAM prior to payment. They will now be able to check SAM sensitive financial data from entity registration records alongside the other Treasury's Working System databases. This will enable agencies to make more informed and efficient payment decisions.

5. There are no additional costs associated with expanding or centralizing access to SAM sensitive financial data from entity registration records because Treasury's Working System already includes this data. As a result, Treasury's Working System already has interfaces in place to allow for access to GSA's existing SAM technology feeds.

6. No additional policy or stakeholder considerations were identified.

Consideration for Designating the Internal Revenue Service's (IRS) Automatic Revocation of Exemption List (ARL)

OMB proposes to designate the IRS's ARL, which maintains records of entities that have lost tax-exempt status due to failure to file an annual information return or notice with the IRS for three consecutive years. The Federal government administers a number of grant programs that pertain specifically to tax-exempt entities. As such, verification against ARL will assist grant-making agencies in verifying tax-exempt status prior to payment.

OMB has reached the following initial determinations and is seeking public comment before finalizing the designation of the database.

1. There are no statutory or other limitations that would prevent including this public database within Treasury's Working System.

2. There are no prohibitive privacy restrictions or risks for Treasury to make this publicly facing database also available in Treasury's Working System. Risk mitigation measures include maintaining a current and compliant SA&A package for Treasury's Working System in accordance with OMB Circular No. A-130. To reduce the likelihood of incidents triggered by unauthorized access, login to Treasury's Working System requires PKI or PIV credentials. All users and administrators are required to sign rules of behavior stipulating their responsibilities to minimize risks and support DNP's mission to "Protect the integrity of the government's payment process by assisting agencies in mitigating and eliminating improper payments in a cost-effective manner while safeguarding the privacy of individuals." In this vein, Treasury has also dedicated resources to establish a Privacy Program based on applicable requirements, FIPPs, and industry best practices. This Treasury's Privacy Program champions various internal controls in concert with agency leadership and counsel such as a data usage governance process charged with vetting projects that support foster a data driven approach to reducing improper payments for Treasury's specific customers and government-wide.

3. Designating IRS' ARL would likely strengthen program integrity. With access to this database through Treasury's Working System, an agency will be better equipped to minimize the risk that it makes a payment to an entity that has not had its tax-exempt status verified.

4. It would be beneficial to streamline access to the ARL through its inclusion within Treasury's Working System. Many of DNP's customers are grant-issuing agencies. This will enable agencies to make more informed payment decisions, increase efficiency, and strengthen internal controls.

5. Aside from budgeted system development costs, there are no additional costs associated with expanding or centralizing access to this publically available database within Treasury's Working System.

6. No additional policy or stakeholder considerations were identified.

Consideration for Designating the IRS's Exempt Organizations Select Check (EO Select Check)

OMB proposes to designate the IRS's EO Select Check, which maintains records of organizations eligible to receive tax-deductible charitable contributions. IRS Publication 78 requires organizations with gross receipts over $50,000 to file Form 990 once every three years in order to remain eligible for tax-exempt status. The EO Select Check database is even more valuable when used in concert with ARL, and will allow agencies to verify an entity's tax-exempt status prior to payment.

OMB has reached the following initial determinations and is seeking public comment before finalizing the designation of the database.

1. There are no statutory or other limitations that would prevent including this public database within Treasury's Working System.

2. There are no prohibitive privacy restrictions or risks for Treasury to make this publicly facing database also available in Treasury's Working System. Risk mitigation measures include maintaining a current and compliant SA&A package for Treasury's Working System in accordance with OMB Circular No. A-130. To reduce the likelihood of incidents triggered by unauthorized access, login to Treasury's Working System requires PKI or PIV credentials. All users and administrators are required to sign rules of

behavior stipulating their responsibilities to minimize risks and support DNP's mission to "Protect the integrity of the government's payment process by assisting agencies in mitigating and eliminating improper payments in a cost-effective manner while safeguarding the privacy of individuals." In this vein, Treasury has also dedicated resources to establish a Privacy Program based on applicable requirements, the FIPPs, and industry best practices. This Treasury's Privacy Program champions various internal controls in concert with agency leadership and counsel such as a data usage governance process charged with vetting projects that support foster a data driven approach to reducing improper payments for Treasury's specific customers and government-wide.

3. Designating IRS's EO Select Check database would likely strengthen program integrity. With access to this database through Treasury's Working System, an agency will be better equipped to minimize the risk that it makes a payment to an entity that has not had its tax-exempt status verified.

4. It would be beneficial to streamline access to the EO Select Check through its inclusion as an additional database within Treasury's Working System. Many of DNP's customers are grant issuing agencies. This will enable agencies to make more informed payment decisions, increase efficiency, and strengthen internal controls.

5. Aside from budgeted system development costs, there are no additional costs associated with expanding or centralizing access to this publically available database within Treasury's Working System.

6. No additional policy or stakeholder considerations were identified.

<u>Consideration for Designating the IRS's e-Postcard</u>

OMB proposes to designate the IRS's e-Postcard database, which maintains records of small entities eligible to receive tax-deductible charitable contributions. Entities within e-Postcard are considered both small businesses and tax-exempt, with gross receipts under $50,000. These organizations are required to file a Form 990-N once every three years in order to remain eligible for tax-exempt status. As with the EO Select Check database, e-Postcard will allow agencies to verify tax-exempt status before making a payment.

OMB has reached the following initial determinations and is seeking public comment before finalizing the designation of the database.

1. There are no statutory or other limitations that would prevent including this public database within Treasury's Working System.

2. There are no prohibitive privacy restrictions or risks for Treasury to make this publicly facing database also available in Treasury's Working System. Risk mitigation measures include maintaining a current and compliant SA&A package for Treasury's Working System in accordance with OMB Circular No. A-130. To reduce the likelihood of incidents triggered by unauthorized access, login to Treasury's Working System requires PKI or PIV credentials. All users and administrators are required to sign rules of behavior stipulating their responsibilities to minimize risks and support DNP's mission to "Protect the integrity of the government's payment process by assisting agencies in mitigating and eliminating improper payments in a cost-effective manner while safeguarding the privacy of individuals." In this vein, Treasury has also dedicated resources to establish a Privacy Program based on applicable requirements, the FIPPs, and industry best practices. This Treasury's Privacy Program champions various internal

controls in concert with agency leadership and counsel such as a data usage governance process charged with vetting projects that support foster a data driven approach to reducing improper payments for Treasury's specific customers and government-wide.

3. Designating IRS' e-Postcard database would likely strengthen program integrity. With access to this database through Treasury's Working System, an agency will be better equipped to minimize the risk that it makes a payment to an entity that has not had its tax-exempt status verified.

4. It would be beneficial to streamline access to the e-Postcard through its inclusion as additional database within Treasury's Working System. Many of DNP's customers are grant issuing agencies. This will enable agencies to make more informed payment decisions, increase efficiency, and strengthen internal controls.

5. Aside from budgeted system development costs, there are no additional costs associated with expanding or centralizing access to this publically available database within Treasury's Working System.

6. No additional policy or stakeholder considerations were identified.

Considerations for Designating American InfoSource (AIS) Deceased Data

OMB has considered Treasury's recommendation and assessment of the suitability of AIS Deceased Data for designation within Treasury's Working System. OMB proposes to designate AIS Deceased Data for inclusion in Treasury's Working System. Treasury's suitability assessment, which evaluates the suitability of AIS Deceased Data, is attached.

Highlights of Treasury's assessment on AIS Deceased Data against the considerations and factors outlined in Section 5(b) of OMB Memorandum M-13-20 follow:

1. There are no statutory or other limitations that would prevent Treasury from using or sharing AIS Deceased Data through Treasury's Working System.

2. Treasury assessed privacy restrictions and risks by reviewing AIS' responses to a questionnaire based on Federal Trade Commission (FTC) vendor management guidance and conducting a data source profile. The information AIS provided regarding data restrictions and risks helped inform Treasury's decision to request this OMB designation of AIS.

The questionnaire includes sections on Products and Services, Breach Notification, Consumer Access and Redress, and Legal Action/Complaints/Inquiries. AIS' response indicated that there are no consumer access or redress procedures in place because their data is not directly acquired from the consumer. AIS data is gathered through public records and additional data sources. AIS maintains that policies, practices and procedures relating to the monitoring, auditing, or evaluation of the accuracy of personally identifiable information may be customized and approved by Treasury as its customer.

Treasury evaluated AIS Deceased Data in various areas, including a data quality assessment at the attribute level, and at the level of the source as a whole. Per-data element measures include quantifications of accuracy, coverage, and conformity. Whole-source measures include assessments of the freshness, completeness, and uniqueness of all records. These six assessments factors, some of which are multi-part, reduce to six

quantitative scores, and these six scores are combined into an overall data source quality benchmark. The quality assessment was performed on a snapshot of the data source from July 14, 2014, for December and January deaths and from March 28, 2014, for November deaths.

3. Designating AIS Deceased Data will strengthen program integrity. Treasury performed an analysis, in which it was conservatively estimated, that the program's use of just three months of AIS Deceased Data would have resulted in the identification of 226 additional improper payments, with a corresponding reduction of roughly $450,000 in improper payments to deceased persons. Please see sections IV(A)(5) and IV(B)(2) of the AIS Deceased Data suitability assessment for more detail on the results of this analysis.

4. Streamlining Federal officials' access to AIS Deceased Data as an additional database within Treasury's Working System supports the Administration's objectives to reduce duplication and costs to taxpayers. Adding in this needed data source without streamlining through Treasury would require each agency to purchase the data set separately, resulting in delays to access and redundant.

5. There will be some additional costs associated with expanding or centralizing access to AIS Deceased Data. However, Treasury has performed a trial assessment with respect to AIS Deceased Data, and has determined that the return on investment (ROI) is positive and outweighs the costs. Please see sections IV(A)(5) and IV(B)(2) of the AIS Deceased Data suitability assessment for more detail on how this analysis was performed and the results.

6. No additional policy or stakeholder considerations were identified.

We invite public comments on the proposed designation of each of the six databases described in this notice.

_____

Mark Reger
Deputy Controller

Do Not Pay: Written Assessment of the Suitability of the AIS Deceased Data Commercial Database

The Office of Management and Budget (OMB) Memorandum M-13-20 requires the Department of the Treasury to prepare and submit to OMB a written assessment to document the suitability of any commercial database proposed for use in Treasury's Working System. Section 11(d) of M-13-20 requires the assessment to address four topics:

(i) the need to use or access the data;

(ii) how the data will be used or accessed;

(iii) a description of the data, including each data element that will be used or accessed; and

(iv) how the database meets all applicable requirements of M-13-20.

Treasury has completed its assessment of the suitability of American InfoSource (AIS) Deceased Data for inclusion as a database in Treasury's Working System. Based on its assessment, Treasury recommends that OMB propose the inclusion of AIS Deceased Data into Treasury's Working System. Below are Treasury's evaluations and conclusions regarding the Section 11(d) topics.

I. Explanation of the need to use or access the data

Decedent persons are ineligible to receive payments with few exceptions, such as to payments to survivors under the deceased name or payments to an estate for work completed before death. As such, the deceased are ineligible for most benefits, grants, or awards. There is a business need for the government to use the most complete, timely, and accurate data to ensure an improper payment is not made to these persons. Currently, government sources of death data include the Social Security Administration's (SSA) Death Master File (DMF), the Centers for Disease Control and Prevention's (CDC) National Vital Statistics System, and data maintained by the Internal Revenue Service (IRS) derived from Table 2000CM of tax returns.

The AIS Deceased Data database includes information about deceased persons from all 50 states. AIS Deceased Data provides death data from states currently unavailable to Treasury customers through SSA's DMF. Treasury's Working System currently uses the public version of SSA's DMF. There is also a restricted version of DMF (known as the "public plus state" DMF), which is more comprehensive and contains more data reported from states than the public version. The Social Security Act limits the disclosure of state death records contained in the "public plus state" DMF to only benefit paying agencies. SSA has determined that Treasury's Working System does not meet the requirements for access to the "public plus state" DMF. Therefore, Treasury evaluated the coverage of AIS Deceased Data by state "public plus state" DMF and found that AIS does have significant coverage in many states above and beyond public DMF which are not contained within "public plus state" DMF. In addition to inputs from SSA's public DMF,

AIS gathers information from probate court records and published obituaries. Obituaries are obtained by AIS from over 3,000 funeral homes and thousands of newspapers, and probate records are collected from the county courts. These sources are not currently available to agencies accessing Treasury's Working System. Out of 600,000 records Treasury received from AIS when assessing the suitability of the database, approximately 230,000 came from sources (obituaries and probationary records) other than the public version of DMF. The positive return on investment (ROI) analysis (Section IV) removed DMF files from its calculations further supporting that including records from AIS in Treasury's Working System will create value to Federal agencies that require this additional death data to make payment decisions.

II. Explanation of how the data will be used or accessed

Generally, when payment-issuing agencies identify a business need to match against a specific type of database, Treasury will work with the payment-issuing agency to complete an Initial Questionnaire. An Initial Questionnaire is the form that Treasury must approve for each payment-issuing agency to initiate the onboarding process, and begin the process of accessing the requested databases. The objectives of the onboarding process are to:

- Allow the payment-issuing agency to gain access to Treasury's Working System;
- Outline business needs and legal authorities for the payment-issuing agency to access Treasury's Working System; and
- Ensure that payment-issuing agency files are ready for use in Treasury's Working System.

During the onboarding process, if an agency determines it has a business need to access death data like AIS Deceased Data – typically, to assist the agency in making eligibility determinations for payments or awards, customers will also identify the method by which their agency will search, or be disclosed, AIS Deceased Data (via online single search, batch matching, continuous monitoring, DNP Analytics, or a combination of these services). To access the batch matching and continuous monitoring matching functions, customers must establish a secure file transfer process with Treasury. Treasury then works with customers to provision access credentials and obtain supplementary information necessary to access Treasury's Working System. Each customer must certify and agree to Rules of Behavior for Treasury's Working System and certify and execute several legal agreements. Customers will then identify AIS Deceased Data as the specific database relevant to their matching needs.

Upon obtaining access to use Treasury's Working System, a comparison between AIS data and agency payment data could be made, resulting in the return of positive matches. Users may either use Treasury's online portal to view automated match results on a regular basis, or request analytical services to be performed in order to gain additional insight. It is then the customer's responsibility to review the information received and make a determination, or request additional services.

III. Description of the data (including each data element that will be used or accessed)

Data Element Definitions

Header	Description of Data	Related Fields in DMF
Last Name	The last name of the deceased individual.	lastname
First Name	The first name of the deceased individual.	firstname
Middle Name	The middle name of the deceased individual.	middlename
City	The city of residence for the deceased individual.	-
State	The state of residence for the deceased individual.	-
Social Security Number (SSN)	A 9-digit identification number used by the SSA. It is exclusively issued by SSA and is predominantly used for the individual classification.	ssn
Date of Death (Dod)	The date of death for the deceased individual, used to determine if payment date is before or after death date.	dateofdeath
Date of birth (Dob)	The date of birth for the deceased individual, which is a supplemental matching element payment-issuing agencies may use as an additional unique identifier to increase confidence in match accuracy.	dateofbirth
Acquired[5]	Identifies when the data was first acquired by AIS.	-
Age	Identifies the number of days between the acquired date and the date of death.	-
Confidence	Level of confidence in the data within the record, determined by the source of the death report (DMF, probate court, obituary, and/or independent verification by AIS).	verifyproof_cd
Source count	The number of death sources in which the record was found.	-
Source	The source from which the record was first acquired.	-

[5] The Acquired and Age data elements reflect the timeliness of the data, and document when AIS compiled the specific death record.

IV. Explanation of how the database meets all the applicable requirements of OMB M-13-20

M-13-20 outlines three distinct sets of requirements for including additional databases in Treasury's Working System.

A. M-13-20 Section 5(b) – Considerations for Designation of Additional Databases

M-13-20 section 5(b) requires that when considering additional databases for designation, OMB will consider:

1. Statutory or other limitations on the use and sharing of specific data;
2. Privacy restrictions and risks associated with specific data;
3. Likelihood that the data will strengthen program integrity across programs and agencies;
4. Benefits of streamlining access to the data through the central DNP Initiative;
5. Costs associated with expanding or centralizing access, including modifications needed to system interfaces or other capabilities in order to make data accessible; and
6. Other policy and stakeholder considerations, as appropriate.

Treasury has assessed AIS Deceased Data against the considerations and factors outlined in Section 5(b) of M-13-20. Treasury has determined that:

1. There are no statutory or other limitations that would prevent Treasury from using or sharing AIS Deceased Data through Treasury's Working System.

2. Treasury assessed privacy restrictions and risks by reviewing AIS' responses to a questionnaire based on Federal Trade Commission (FTC) vendor management guidance and conducting a data source profile. These inputs that considered data restrictions and risks informed Treasury's decision to request this designation request.

   The questionnaire includes sections on Products and Services, Breach Notification, Consumer Access and Redress, and Legal Action/Complaints/Inquiries. AIS' response indicated that there are no consumer access or redress procedures in place because their data is not directly acquired from the consumer. AIS data is gathered through public records and additional data sources. AIS maintains that policies, practices and procedures relating to the monitoring, auditing, or evaluation of the accuracy of personally identifiable information may be customized and approved by the Treasury as its customer.

   Treasury evaluated AIS Deceased Data in various areas, including a data quality assessment at the attribute level, and at the level of the source as a whole. Per-data element measures include quantifications of accuracy, coverage, and conformity. Whole-source measures include assessments of the freshness, completeness, and uniqueness of all records. These six assessments factors, some of which are multi-part, reduce to six quantitative scores, and these six scores are combined into an overall data source quality benchmark. The quality assessment was performed on a snapshot of the data source, from July 14, 2014 for December and January deaths and from March 28, 2014 for November deaths.

3. Designating AIS Deceased Data will strengthen program integrity. Treasury performed an analysis in which it was conservatively estimated that the program's use of just three months of AIS Deceased Data would have resulted in the identification of 226 additional improper payments, with a corresponding reduction of roughly $450,000 in improper payments to deceased persons. Please see section IV(A)(5) and IV(B)(2) for more detail on how this analysis was performed and the results.

4. It is beneficial to the Federal government and to taxpayers to streamline access to AIS Deceased Data as an additional database within Treasury's Working System. Currently, in order to access AIS Deceased Data, customer agencies must each procure the data themselves. This process can take up to six months to complete and is costly and duplicative. With over 140 programs currently accessing Treasury's Working System, the amount of time saved with a single procurement will have a positive ROI.

5. There will be some additional costs associated with expanding or centralizing access to AIS Deceased Data. However, Treasury has performed a trial assessment with respect to AIS Deceased Data, and it has determined that the ROI is positive and outweighs the costs. Specifically, the trial assessment compared three months of AIS data to current and historical payment data in order to determine which payments would result in matches. Agency-specific business rules identified in Treasury's current processes were then applied to reduce false positives. ROI was 400%. Recurring payments were then eliminated to simulate

an agency stopping the first payment, thus nullifying benefit from future payments. ROI was found to be 315%.

6. No additional policy or stakeholder considerations were identified.

B. M-13-20 Section 11(b) – General Standards for the Use or Access to Commercial Databases

M-13-20 Section 11(b) provides that Treasury may use or access a commercial database for Treasury's Working System only if OMB has officially, previously designated such database for inclusion following a period of public notice and comment, as described in section 5(b) of this Memorandum. Because commercial databases used or accessed for purposes of the DNP Initiative will be used to help agencies make determinations about persons, it is important that agencies apply safeguards that are similarly rigorous to those that apply to systems of records under the Privacy Act. Thus, commercial data may only be used or accessed for the DNP Initiative when the commercial data in question would meet the following general standards:

1. Information in commercial databases must be relevant and necessary to meet the objectives described in section 5 of IPERIA.
2. Information in commercial databases must be sufficiently accurate, up-to-date, relevant, and complete to ensure fairness to the individual record subjects.
3. Information in commercial databases must not contain information that describes how any individual exercises rights guaranteed by the First Amendment, unless use of the data is expressly authorized by statute.

Treasury has assessed AIS Deceased Data against the considerations and factors outlined in Section 11(b) of M-13-20. Treasury has determined that:

1. AIS Deceased Data is relevant and necessary to meet objectives set out in the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA). IPERIA requires payment-issuing agencies to verify eligibility of payments and awards by reviewing the SSA DMF, as appropriate. Treasury has access to the public DMF, but does not currently have access to the "public plus state" DMF or probate court records and obituaries. AIS Deceased Data provides the latter two categories, creating value for payment-issuing agencies in this additional death data. Additionally, AIS Deceased Data includes records from states, including 18 states that do not report deaths to SSA via the Internet Electronic Death Registration (I-EDR), and would not be included in the "public plus state" DMF anyway. AIS Deceased Data will supplement the existing data provided by SSA in the public DMF and further inform the payment decisions of Treasury customers.

2. In its trial assessment, Treasury determined that AIS Deceased Data is sufficiently accurate, up-to-date, relevant, and complete to ensure fairness. Treasury compared the AIS Deceased Data city and state data to other databases that are considered "gold standards" and over 99 percent of these data were accurate. Treasury also assessed AIS Deceased Data social security number (SSN), date of death, and date of birth data elements and determined that: over 99 percent of the SSN data are accurate; all records contain a date of death; and 89 percent of the data contain a date of birth, which is sufficiently accurate for a supplemental matching element. The data elements that AIS will provide to Treasury's Working System all directly relate to confirming the identification of a person's

status as deceased and would be fully refreshed on a quarterly basis. Extraneous fields are not included to ensure that data minimization standards (see M-13-20 section 5(c)) are applied. In addition, Treasury only receives records from AIS, which contain a SSN, first name, and last name. These practices and the data elements will ensure fewer false positives and fairness to the record subjects.

3. AIS Deceased Data does not contain information that describes how an individual exercises rights guaranteed by the First Amendment.

C. M-13-20 Section 11(c) – Specific Requirements for Use or Access to Commercial Databases

M-13-20 Section 11(c) provides that in addition to the general standards provided above, Treasury shall meet the following specific requirements whenever agencies use or access a commercial database as part of Treasury's Working System:

1. Treasury shall establish rules of conduct for persons involved in the use of or access to commercial databases and instruct each person with respect to such rules, including penalties for noncompliance, as appropriate.
2. Treasury shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of information in commercial databases when such information is under Treasury's control.

Treasury has assessed AIS Deceased Data against the considerations and factors outlined in Section 11(c) of M-13-20. Treasury has determined that it has fulfilled the requirements of Section 11(c) because:

1. Treasury has established rules of conduct for users of the Treasury's Working System. Users must agree to the following:

    - To use information to perform job duties and to only access data necessary to perform said duties;
    - To not use data for fraud;
    - To not browse or access data without authorization;
    - To make no changes to data delivered;
    - To not use data for personal gain;
    - To report conflicts of interest immediately;
    - To terminate access when access is no longer required for job duties; and
    - To not disclose information to unauthorized persons.

    Terms and conditions which must be accepted each time a customer accesses the Treasury's Working System include a description of penalties for misuse of data. These include:

    - criminal and civil penalties
    - disciplinary actions and other consequences including the loss of system access

2. Treasury has strong safeguards to protect the security and confidentiality of information. Access to the Treasury's Working System is available only by authorized persons on a need-to-know basis. External access logs to Treasury's Working System are reviewed to ensure compliance with the Rules of Behavior agreed to by credentialed users. Internal access log control measures are

reviewed to ensure compliance with security guidelines governing access to Privacy Act data. Audit logs allow system managers to monitor external and internal user actions and address any misuse or violation of access privileges. Access to computerized records is limited through the use of internal mechanisms available to only those whose official duties require access. Facilities where records are physically located are secured by various means, such as security guards, locked doors with key entry, and equipment requiring a physical token to gain access. The Bureau of the Fiscal Service may agree to additional safeguards for some data through a written agreement with the entity supplying the data.

Treasury's Working System recently completed its Security Assessment and Authorization (SA&A), which is reviewed at the Bureau of the Fiscal Service level. The SA&A adheres to the processes outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series. More specifically, NIST SP 800-115; NIST SP 800-53, Rev. 3; NIST SP-800-53A, Rev. 1; NIST SP 800-37, Rev. 1; and NIST SP 800-30. Treasury's Working System also complies with the Federal Information Security Management Act (FISMA). For example, detailed SA&A information is currently safeguarded within the Treasury FISMA Information Management System; in the event of an audit, this documentation may be made available.

[FR Doc. 2017-19433 Filed: 9/12/2017 8:45 am; Publication Date: 9/13/2017]